

Laptops

- Store your laptop in a locked cabinet or room when it is not in use.
- Don't store confidential or sensitive data without using approved encryption software when the software is available.
- Laptop displays should be positioned to preclude casual viewing by others, especially when confidential or sensitive data is shown on the display.
- Always store and transport your laptop in its carrying case.
- Avoid storing laptops in aircraft overhead compartments.
- While traveling, keep the laptop and peripheral equipment with you whenever possible.
- If you must leave the laptop, store it securely out of sight.
- Avoid leaving a laptop in a vehicle. If you must store the laptop in a vehicle, lock it in the trunk.
- Hand-check the laptop or put it through the X-ray machine when going through airport security. *Keep all equipment in view at all times until you retrieve it. Thieves may attempt to distract you to steal the laptop.*
- If you encounter problems with the laptop, do NOT attempt to repair it yourself.
- When using laptops to connect to networks, only connect to systems you are authorized to use.
- Always logoff from network connections during periods of inactivity.

For More Information

For more information on Internet and e-mail usage, backups, password controls, laptop security and viruses, please refer to the following CDSS Information Security Policies available on the CDSS internal Web page:

- Internet and E-Mail Usage Policy
- E-mail Retention Policy
- Employee Password Controls Policy
- Personal Computer Administrator Password Controls Policy
- System Administrator Password Controls Policy
- Guidelines For Password Protection And Security
- Frequently Asked Questions About Passwords
- Password Controls Policies Implementation Plan
- Backup Policy
- Guidelines For Identifying Necessary Data
- Guidelines For Establishing A Backup Process
- Guidelines For Choosing A Backup Process
- Virus Protection Policy
- Frequently Asked Questions about Viruses
- Laptop Security Policy
- Glossary

Questions?

Call the Information Security and Management Systems Branch at 657-3409

State of California

Gray Davis, Governor

Health and Human Services Agency

Grantland Johnson, Secretary

Department of Social Services

Rita Saenz, Director



Good Information Security Practices

- Use State computer equipment, computer systems, networks (including the Internet) and e-mail only for work-related activities. *They are not to be used for personal use.*
- Keep food and drink away from computer equipment.
- Politely question unauthorized, unfamiliar persons in your work area.
- Share confidential or sensitive information only with persons who have a documented “need to know”.
- Clearly label sensitive or confidential documents and storage media. Store them in a secure environment.
- Terminate access to CDSS computer systems and networks when staff leave the Department.
- Limit access to specialized CDSS computer systems to persons that have a work-related need.

Internet and E-Mail Usage

- Your use of the Internet and e-mail is not private. Activity records can be monitored and recovered by the State (even after you have deleted them).
- Your e-mail may be subject to public disclosure under the Public Records Act.
- Always confirm the correct e-mail address of the intended receiver.
- Don’t e-mail confidential or sensitive information without approved encryption software.
- Don’t conduct or engage in any illegal or prohibited activities.
- Don’t send or forward junk mail or chain letters.

Passwords

- Use passwords with 7 or more characters using a random mix of numbers and letters.
- Use a different password for your PC (power-on password) than the password for your network, applications or operating system.
- Use a phrase to help you remember your password.
- Don’t use a password that is in a dictionary or that somebody can guess.
- Don’t reveal your passwords to anyone other than your Supervisor or his/her designee.
- Don’t write down your passwords.
- Change your passwords every 90 days or whenever you suspect they’ve been compromised.

Virus Protection

Warning signs of a suspected virus:

- Your computer or software acts unusual (your file looks like it is “melting” or strange shapes appear).
- Your file size, date or time are inaccurate.

Things to do to protect yourself:

- Ensure that you have activated anti-virus software that is regularly upgraded (to protect against new viruses), configured to provide the maximum level of protection and configured to perform automatic scans of your hard disk once a week.
- Always scan software disks and files with approved anti-virus software.

What to do if you suspect a virus:

- Immediately stop using your PC.
- Notify your Supervisor.

Backups

What data should be backed up?

- Confidential, sensitive and mission-critical data or data that you don’t want to lose.

What data is already backed up?

- Data that is (1) stored on an ISD-owned server (such as the Sun, Motorola, MIDAS, etc.), (2) stored on a Data Center – managed system (e.g. SAWS, or CWS/CMS, etc.) or (3) backed up through a contractual arrangement. In these cases, your backup needs are taken care of for you. For questions, see your Personal Computer Administrator (PCA).

Backup Basics

- Backup your data regularly, in accordance with your unit’s backup procedures.
- Store all original software diskettes in a safe place and where they can be obtained quickly to recover from minor events (such as accidental deletion of files).
- Always keep your backups stored safely.
- Regularly test your backups.
- Keep similar information together in the same directory.
- Data files, application files, and system files should be kept in separate directories.
- Give logical names to your documents, directories and subdirectories.
- Keep backup copies in off-site storage (another building) for use following a disaster.
- Never store backups at your home.
- Maintain at least three generations of backups.